UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/914,258	02/08/2002	Andrew Augustine Wajs	5683P013	2221

21186 7590 04/04/2006

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH
121 S. 8TH STREET
SUITE 1600
MINNEAPOLIS, MN 55402

EXAMINER	
SZYMANSKI, THOMAS M	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 04/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/914,258	WAJS ET AL.	
	Examiner	Art Unit	
	Thomas Szymanski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-3,5 and 7* is/are allowed.

6)☒ Claim(s) *4,6,8 and 9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02/08/2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9 have been examined.

Drawings

2. In view of the applicant's arguments the examiner has re-considered the drawings and withdrawn the previously presented objection.

Specification

3. The objections to the specification are withdrawn in view of the applicant's amendments.

Claim Rejections - 35 USC § 112

4. Previously presented rejections under this section have been overcome by the applicant's amendments.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claims 4 and 8 are rejected under 35 U.S.C. 102(a) as being anticipated by International application published under the PCT, WO 99/19822 Birdwell et al. ("Birdwell").

7. Regarding Claim 4: conditional access system comprising a number of subscribers (Fig 1-4, pg 1 lines 17-20, pg 5 lines 15-24)

Each-subscriber having a terminal including a conditional access module and a secure device to store entitlements (Fig 1-4, pg 12 lines 23-24) As shown each client has a secure memory and access module for receiving the content.

A source signal is encrypted using a first key and broadcast for receipt by terminals, first key is changed at a high rate (Fig 1, pg 7 lines 3-10, pg 16 lines 19-20, pg 18 lines 1-25) Birdwell et al teaches changing the keys at a high rate within the suspected group in relation to finding the pirated terminal. Additionally, a first key within the scope of a conditional broadcast system is always changed at a high rate.

Entitlement control messages (ECM's) are sent to the secure devices, comprising the first key encrypted using a service key (pg 5 lines 15-18, Fig 5-7, pg 8 line 20-pg 9 line 2) This system is implemented within a conditional broadcast system as specified, it is well known within such a system that these messages containing the specified encrypted keys are ECM's.

Entitlement management messages (EMM's) are sent to the secure device providing the service key required to decrypt encrypted first keys (Fig 5-6, pg 8 line 20-pg 9 line 2) As stated by Birdwell et al and as denoted above the session keys are encrypted by an authorization key (service key) that is distributed to the client.

A cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate (pg 15 line 21-pg 16 line 15)

Search EMM'S are sent to at least a part of the terminals (pg 16 lines 1-15) As stated the system provides a search message methodology to track down the pirated terminal. Each search EMM of the set comprising a different dummy key (Po) and each EMM being sent to a different part of the terminals (Fig 7, pg 16 lines 9-14) As shown by Birdwell et al within a specified embodiment a different key or dummy key is sent to each involved party.

8. Regarding Claim 8: The distribution of the terminals in groups of terminals is varied to trace the cracked secure device (Birdwell Fig 7, pg 17 line 20 – pg 19 line 20)

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 6 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomson Multimedia EP 0822720A1, and further in view of Birdwell et al WO 99/19822 ("Birdwell").

11. Thomson Multimedia teaches a conditional access system that encrypts the first key or control word many different times using a plurality of different keys. (Fig 3a, 3b, Col 6 line 51 – Col 9 line 15)

12. Thomson Multimedia fails to teach tracing pirated terminals through the use of distributed key shares.

13. Birdwell et al discloses a conditional access system for the tracking of pirated terminals by distribution of specific authorization keys to different groups. (pg 15 line 21 – pg 17 line 19)

14. It is desirable within any system to maintain a high level of security and to have the ability to maintain services without the theft of those services occurring and individuals pirating such services through the distribution of sensitive system information. (Birdwell pg 1 line 11 – pg 2 line 19)

15. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the tracking system of Birdwell et al into that of Thomson Multimedia for the advantages of improved system security.

16. Regarding Claim 6: conditional access system comprising a number of subscribers (Birdwell et al Fig 1-4, pg 1 lines 17-20, pg 5 lines 15-24)
Each-subscriber having a terminal including a conditional access module and a secure device to store entitlements (Birdwell et al Fig 1-4, pg 12 lines 23-24) As shown each client has a secure memory and access module for receiving the content.

A source signal is encrypted using a first key and broadcast for receipt by terminals, first key is changed at a high rate (Birdwell et al Fig 1, pg 7 lines 3-10, pg 16 lines 19-20, pg 18 lines 1-25) Birdwell et al teaches changing the keys at a high rate within the suspected group in relation to finding the pirated terminal. Additionally, a first key within the scope of a conditional access system is always changed at a high rate.

Entitlement control messages (ECM's) are sent to the secure devices, comprising the first key encrypted using a service key (Birdwell et al pg 5 lines 15-18, Fig 5-7, pg 8 line 20-pg 9 line 2) This system is implemented within a conditional broadcast system as specified, it is well known within such a system that these messages containing the specified encrypted keys are ECM's.

Entitlement management messages (EMM's) are sent to the secure device providing the service key required to decrypt encrypted first keys (Birdwell et al Fig 5-6, pg 8 line 20-pg 9 line 2) As stated by Birdwell et al and as denoted above the session keys are encrypted by an authorization key (service key) that is distributed to the client.

17. A cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate (Birdwell et al pg 15 line 21-pg 16 line 15)

18. The source signal or the ECM's are encrypted using a multiple-key or secret-sharing cryptographic algorithm having a plurality of different decrypting keys or shares required for decrypting the encrypted source signal or ECM'S respectively (Thomson Multimedia Fig 3a, 3b) As shown the keys are in the format of a share in the respect

that each key is associated by the union of the group to share the decrypting of the data, so thereby providing for such a share of the decrypting.

Plurality of different decrypting keys or shares (Ci;Pi) are sent to at least a part of the terminals such that different terminals or groups of terminals receive different keys or shares according to a predetermined distribution. (Thomson Col 6 line 51 – Col 9 line 15, Birdwell pg 16 lines 9-14) As stated within the Thomson Multimedia document the control words are encrypted with a plurality of different authorization keys and as provided for by Birdwell et al and Thomson these keys are distributed according to a desired pattern amongst the terminals.

19. Regarding Claim 9: The distribution of the terminals in groups of terminals is varied to trace the cracked secure device (Birdwell Fig 7, pg 17 line 20 – pg 19 line 20)

Response to Arguments

20. Applicant's arguments filed 02/09/2006 have been fully considered but they are not persuasive.

21. In regards to applicant's argument of the differences between dummy key as used by the applicant and as anticipated by Birdwell, the recitation of dummy key within the applicant's claim does not differentiate itself from the multiple keys as used by Birdwell. The additional process of sending out search EMM's by Birdwell is easily characterized as using a dummy key in the sense of deviating from the typical method of distributing keys and using an additional key (dummy key) over the regular method of distribution to locate a pirate.

22. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

23. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. The applicant has provided no direct evidence against the combination of references but has instead relied upon arguments toward claim 4 to show the novelty of claim 6. Such an argument is overcome by the combination and furthermore as responded to above.

Allowable Subject Matter

24. Claims 1-3, 5, and 7 are allowed.

Conclusion

25. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of art disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

27. Inquiries concerning this communication or earlier communications from the examiner should be directed to Thomas M. Szymanski who can be reached at (571) 272-8574. The examiner's normal working schedule is between the hours 8:00am – 4:30pm (EST), Monday – Friday.

28. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques, can be reached at (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

29. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).